[19]中华人民共和国国家知识产权局

[51]Int.Cl[7]
H04L 9/14

[12]发明专利申请公开说明书

[21]申请号 98118731.5

[43]公开日 2000年3月1日

[11]公开号 CN 1246008A

[22]申请日 1998.8.26 [21]申请号 98118731.5

[71]申请人 英业达股份有限公司
地址 台湾省台北市
[72]发明人 张景嵩 任 真 温周斌

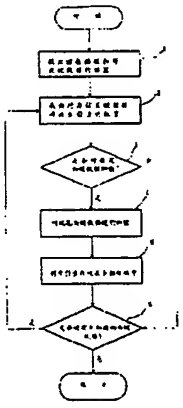
[74]专利代理机构 柳沈知识产权律师事务所
代理人 马 莹

权利要求书2页 说明书5页 附图页数4页

[54]发明名称 多媒体数据的保密方法

[57]摘要

一种多媒体数据的保密方法，具有一加密/解密表，该表分别由一索引值与加 密运算所组成。任一索引值与一种加密运算相对应，利用加密/解密表，对多媒 体数据中的关键数据进行加密/解密，并通过该表中的一种或多种加密运算来 提高加密的可靠性。在加密/解密时，必须同时取得该加密/解密表、该多媒 体数据的关键数据位置以及该加密/解密的索引值，才能进行加密/解密，从 而提高数据保密的可靠性及安全性。



ISSN1008-4274

BEST AVAILABLE COPY

权 利 要 求 书

1. 一种多媒体数据的保密方法，用于对多媒体数据进行加密及解密，该方法包含:

一加密/解密表，该表分别由索引值(index)与加密运算所组成，并且该表中任一索引值与一种加密运算相对应，而且索引值不能重复出现;

在对多媒体数据进行加密的过程中，通信双方预先约定在传送的一种多媒体数据中需要加密的关键数据，而且所述多媒体数据由多个帧组成；其中所述加密过程包含如下步骤:

(1)首先，找出所述数据中除第一个帧外的任一帧内欲加密的关键数据位置;

(2)找出对应所述关键数据的可用来存放索引值的位置;

(3)选择是否对所述关键数据加密，若不加密，则进到步骤(6)，若加密则继续;

(4)从所述加密/解密表中随机选择一数据，作为加密的索引值，并根据所述加密/解密表内索引值所对应的加密运算，对所述关键数据进行加密;

(5)再将所选的索引值存放在所述数据的多个帧中;

(6)判断是否还有未加密的关键数据，若是则回到步骤(2)，若否则全部加密结束;

在对所述加密的多媒体数据解密的过程中，利用所述索引值，对照查出所述表中的加密运算，以进行解密；其中所述解密过程包含如下步骤:

(1)首先，找出所述数据中任一帧内待解密的关键数据位置;

(2)找出对应该关键数据的索引值的存放位置;

(3)再找出被加密覆盖后索引值位置上原先的原始数据，即第一个帧中的数据;

(4)将加密索引值与原始数据作比较，若相同，则表示所述关键数据并未加密，则到步骤(6)，若不相同则继续;

(5)根据该加密索引值存放在所述多个帧中的数据，对照加密/解密表查出所述关键数据所采用的加密运算，可得到加密前的原始关键数据，并藉此进行解密，还原被索引值所覆盖的原始数据;

(6)判断是否还有未加密的关键数据，若是，则回到步骤(1)，若否，则全

部解密结束。

2. 如权利要求 1 所述的多媒体数据保密方法，其中所述加密/解密表内的任一索引值的大小不能超过 4 比特所能表示的最大值，即 15，且该加密/解密表不可包含在被加密后的关键数据中，同时，在加密过程中，使用同一张加密/解密表来对音频数据进行加密。

3. 如权利要求 1 所述的多媒体数据保密方法，其中所述音频数据结构的任一帧中都有一主数据起始部(main_data_begin)，作为被加密对象的关键数据，而在该主数据起始部之前，分别在一个欲加密的基本音频数据单元中设有多个比特数据，且设定用所述多个比特来存放加密后的索引值。

4. 如权利要求 3 所述的多媒体音频数据保密方法，其中所述主数据起始部之前的多个比特数据分别为一个比特的标识符(ID)，两个比特的数据层号(Lay)，一个比特的保护位(Protect)，一共四个比特的数据。

5. 如权利要求 1 或 2 所述的多媒体音频数据保密方法，其中该加密/解密表内的任一索引值所对应的加密运算可自行设计，并且随机重复出现，而且该任一索引值所对应的加密运算可相同，亦可各不相同。

说　明　书

多媒体数据的保密方法

本发明涉及一种多媒体数据的保密方法，具体涉及这样一种多媒体数据的保密方法，其中，利用加密/解密表中的一种或多种加密运算进行加密，从而增加对多媒体数据加密的安全性，且加密/解密索引值(index)包含在该数据中，不必占用额外的存储空间储存加密/解密信息。

在现今信息通信领域中，利用多媒体数据作为一种通讯传输的方式，将促进信息通信业的发展。考虑到一般多媒体数据的版权、隐私性或安全性等特殊原因，常常会对其中各种数据进行加密，具体的方法是：(1)对所有数据进行加密；(2)采用非常复杂的算法以防止非法破密，而由于数据的数据量通常非常庞大，且声音需立即播放而无延迟，因此，若采用非常复杂的算法进行加密，将影响数据及声音播放的效果，倘若对所有数据进行加密，不仅将占用相当大的解密信息存储空间，同时，亦非常容易地遭到非法人士的破密，因此，现有的加密方法无法有效地达到对数据进行保密的目的，导致了不安全性，从而造成使用上的困扰。

针对上述现有的各种缺点，本发明的一个目的是提供一种多媒体数据的保密方法，它是一种针对一多媒体数据的快速、有效且简便的加密方法，根据多媒体数据的固有特点仅对其中的关键数据而非所有数据进行加密，以减少计算量，从而能对大量多媒体数据进行快速加密/解密；并且利用加密/解密表中的一种或多种加密方法进行综合加密，从而增加对多媒体数据加密的安全性。

本发明的另一目的是提供一种多媒体数据的保密方法，其中，可自行设计加密运算，与加密/解密表内索引值相对应的加密运算随机重复出现，且索引值彼此间所对应的加密运算可以相同，亦可以各不相同，而且加密运算越多，安全性越高。

为实现本发明的目的，提供了一种多媒体数据的保密方法，用于对多媒体数据进行加密及解密，该方法包含：

一加密/解密表，该表分别由索引值(index)与加密运算所组成，并且该表中任一索引值与一种加密运算相对应，而且索引值不能重复出现；

在对多媒体数据进行加密的过程中，通信双方预先约定在传送的一种多媒体数据中需要加密的关键数据，而且，所述多媒体数据由多个帧组成；其中所述加密过程包含如下步骤：

(1)首先，找出所述数据中除第一个帧外的任一帧内欲加密的关键数据位置；

(2)找出对应所述关键数据的可用来存放索引值的位置；

(3)选择是否对所述关键数据加密，若不加密，则进到步骤(6)，若加密则继续；

(4)从所述加密/解密表中随机选择一数据，作为加密的索引值，并根据所述加密/解密表内索引值所对应的加密运算，对所述关键数据进行加密；

(5)再将所选的索引值存放在所述数据的多个帧中；

(6)判断是否还有未加密的关键数据，若是则回到步骤(2)，若否则全部加密结束；

在对所述加密的多媒体数据解密的过程中，利用所述索引值，对照查出所述表中的加密运算，以进行解密；其中所述解密过程包含如下步骤：

(1)首先，找出所述数据中任一帧内待解密的关键数据位置；

(2)找出对应该关键数据的索引值的存放位置；

(3)再找出被加密覆盖后索引值位置上原先的原始数据，即第一个帧中的数据；

(4)将加密索引值与原始数据作比较，若相同，则表示所述关键数据并未加密，则到步骤(6)，若不相同则继续；

(5)根据该加密索引值存放在所述多个帧中的数据，对照加密/解密表查出所述关键数据所采用的加密运算，可得到加密前的原始关键数据，并藉此进行解密，还原被索引值所覆盖的原始数据；

(6)判断是否还有未加密的关键数据，若是，则回到步骤(1)，若否，则全部解密结束。

由于上述方法的加密/解密索引值包含在数据中，而不必占用额外的存储空间储存加密/解密信息，因此，不会影响多媒体数据及声音播放效果，且在加密/解密时，必须同时取得加密/解密表、多媒体数据的关键数据位置及加密/解密的索引值才能加密/解密，从而提高加密/解密的可靠性，同时增加了安全性。

为了更进一步认识与了解本发明的目的、特点及功能，以下将参照附图对本发明的实施例进行详细说明。附图中：

图 1 为本发明的基本加密/解密表；

图 2 为本发明的数据结构示意图；

图 3 为本发明实施例的 MP3 加密/解密表；

图 4 为本发明的加密操作流程图；

图 5 为本发明的解密操作流程图。

如图 1 、图 2 、图 3 、图 4 及图 5 所示，本发明的多媒体数据之保密方法具有一加密/解密表 10 ，如图 1 所示。该加密/解密表 10 分别由一索引值与加密运算所组成。每个索引值的大小不能超出 4 比特所能表示的最大值，即 15(十进制)，并且每个索引值与一种加密运算相对应。同时，索引值不能重复出现。而且为了安全起见，该加密/解密表 10 不可包含在被加密(即关键数据)后的数据中。同时，在加密过程中，必须同时使用同一张加密/解密表 10 ，而数据可利用该加密/解密表 10 来进行加密；反之，在解密过程中，利用该索引值来对照查出表中的加密运算，以进行解密。

在本发明的多媒体数据加密过程中，通信双方须先约定一种传送数据中必须被加密的关键数据。其中所采用的数据结构如图 2 所示，它具有多个帧，任一帧都有一个主数据起始部④(main_data_begin, 9 比特)。该部分数据④可指出当前帧中实际数据的存放位置。若改变该部分数据④足以影响整个数据。任一个帧中的主数据起始部④就是关键数据，并且是加密对象，而且，在加密/解密表 10 中选择一种加密运算及其对应的索引值存放位置。

如图 2 所示，在任一个帧中的主数据起始部④之前分别设有：①： ID(标识位， 1 比特)；②： Lay(数据层号， 2 比特)；③： Protect (保护位， 1 比特)，一共四个比特的数据。在一个基本的欲加密的数据单元(如一首歌，一段话)中，每个帧中的这四个比特数据均相同。因此，约定用这些数据①、②、③来存放加密后的索引值(当然该索引值大小不能超过 4 比特所能表示的最大值，即 15)。另外，在国际标准 ISO/IEC 11172-3 中有如何找出这些数据①、②、③、④位置的标准算法，由于不是本发明的发明点，所以在此并不赘述。

按照国际标准 ISO/IEC 11172-3 ， Layer 3 所制作的数据属于多媒体数据的一种，以下简称为 MP3 数据。假定现在制作一首 MP3 格式的歌曲的多

媒体数据。制作完以后会发现其数据形式为许多个帧组成。每个帧中的第12比特为ID(从0开始计数),第13， 14比特为Lay,第15比特为Protect。在所有的该首歌的帧中，这 4 个比特的数据都是一样的。因此，保留第一个帧中的这4个比特的数据,以后的每个帧中的ID， Lay， Protect这四个比特数据都可以从第一帧中获得。因此，除第一帧之外的其它帧的这 4 个比特的数据的位置，可利用来存放加密/解密所使用的索引值（ index ）。在解密时，从这 4 个比特中取出索引值，进行解密。而这 4 个比特原来的值就从第一帧中获得。

另外，每一帧中实际的声音数据存放在何处是没有规则的。根据ISO/IEC 11172-3 国际标准，可以在每一个帧中按照标准算法找到一个 9 比特的数据，称为 main_data_begin 。该数据的作用就是指出该帧中实际的声音数据起始于何处。该数据的错误将导致无法还原声音，因此仅对每一帧中该数据项加密就足以达到对整首歌加密的效果。

在此之前，通常对整首歌曲的所有数据采用一种加密方法进行加密。但在播放时因为要对所有数据进行解密，所以一旦解密算法太复杂，就会造成播放的速度跟不上实际声音的速度，造成声音有停顿；而如果采用简单的加密/解密算法，则非常容易被非法破解。因此本发明克服了以上的矛盾，在实际使用中取得了满意的效果。

下面参照图 4 对本发明一实施例的加密方法进行说明:

(1)首先，找出该 MP3 数据的除第一个帧外任一个帧中欲加密的关键数据，即主数据起始部④的位置;

(2)找出对应该关键数据的可用来存放索引值的位置;

(3)选择是否对该关键数据进行加密，若不加密，则进到步骤(6)，若加密则继续;

(4)从如图 3 所示的MP3加密/解密表10'中随机选择一个不大于15且不等于原来 4 比特的数据，作为加密的索引值，并根据该 MP3 加密/解密表10'内索引值所对应的加密运算，对该关键数据进行加密；例如假设索引值是 7 ，其对应的加密运算是将索引值与关键数据相加;

(5)再将该索引值 7 存放在该 MP3 数据的帧中的①： ID 、②： Lay 、③： Protect 这四个比特中;

(6)判断是否还有未加密的关键数据，若是则回到步骤(2)，若否则全部

加密结束。

反之，参照图 5 所示，在解密过程中，本发明实施例的解密方法如下：

(1)首先，找出该 MP3 数据的任一个帧中待解密的关键数据，即主数据起始部④的位置；

(2)找出对应该关键数据的存放索引值的位置，即该帧中的①： ID、②： Lay 、③ Protect 这四个比特；

(3)再找出被加密覆盖后索引值位置上原先的①： ID 、②： Lay 、③ Protect 这四个比特的原始数据，在本实施例中，即为第一个帧中的①： ID 、②： Lay 、③ Protect 的四个比特；

(4)将该加密索引值与原始数据作比较，若相同，则表示该关键数据并未加密，则进到步骤(6)，若不相同则继续；

(5)根据该加密索引值所存放的四个比特数据，对照 MP3 加密/解密表 10'，查出该关键数据所采用的加密运算；在本实施例中，其索引值是 7 ，其对应的加密运算是将索引值与关键数据相加；因此，将该加密的关键数据减去索引值，即可得到加密前的原始关键数据，并据此进行解密；同时，还原被索引值所覆盖的原始数据，即为该帧中的①： ID 、②： Lay 、③ Protect 这四个比特信息；

(6)判断是否还有未解密的关键数据，若有，则回到步骤(1)，若没有，则全部解密过程结束。

在本发明中，所采用的加密运算可自行设计，如图 1 所示。该加密/解密表 10 内的索引值 0 、 1 、 2 所对应的加密运算可随机重复出现，例如索引值 0 与 3 所对应的加密运算可相同，亦可以各不相同。而且加密运算越多，安全性越高。另外，即使非法破密者得到该加密/解密表 10 ，但如果不知道该任一种多媒体数据格式中，哪些数据是关键数据，及其索引值存放在何处，亦将无从下手。

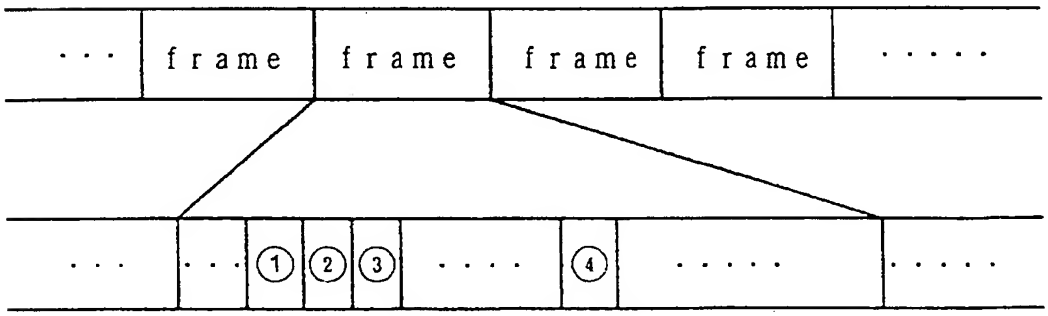
此外，按国际标准 ISO/IEC 13818-3 ， Layer 3 所制作的数据，其帧中的主数据起始部④(11 比特)亦适用于本发明的加密方法。

虽然在上面对本发明的一优选实施例进行了详细说明，但本领域的普通技术人员根据本发明所公开的内容进行的各种等效修饰与变化，均应包括在本发明权利要求书所限定的范围内。

10

索引值	加 密 方 法
0	将被加密数据的各个两进制位取反
1	将被加密数据与此项的索引值做异或
2	将被加密数据加上此项索引值
3	将被加密数据的各个两进值位取反
4	将被加密数据加上此项索引值
.	(某加密方法)
.	(某加密方法)
.	(某加密方法)

图 1



① : ID(1bit)

② : Lay(2bit)

③ : Protect(1bit)

④ : main_data_begin(9bit)

图 2

10

索引值	加密方法
0	将索引值与被加密数异或
1	将索引值与被加密数相加
2	将索引值与被加密数异或
3	将索引值与被加密数相加
4	将索引值与被加密数相加
5	将索引值与被加密数异或
6	将索引值与被加密数相加
7	将索引值与被加密数相加
8	将索引值与被加密数相加
9	将索引值与被加密数相加
10	将索引值与被加密数相加
11	将索引值与被加密数异或
12	将索引值与被加密数相加
13	将索引值与被加密数相加
14	将索引值与被加密数异或
15	将索引值与被加密数相加

图 3

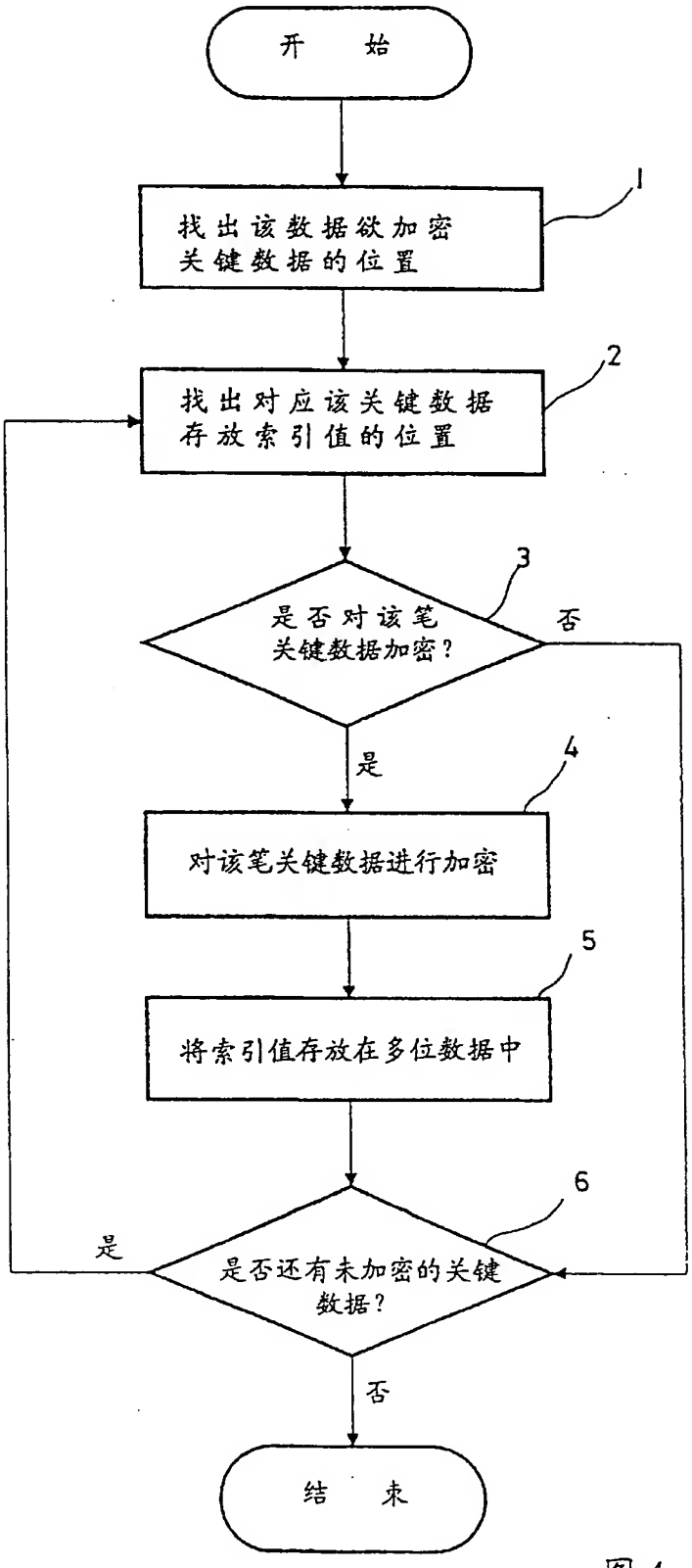

开 始
找出该数据欲加密关键数据的位置
1
找出对应该关键数据存放索引值的位置
2
是否对该笔关键数据加密？
3
否
是
对该笔关键数据进行加密
4
将索引值存放在多位数据中
5
是否还有未加密的关键数据？
6
是
否
结 束

图 4

98-08-26

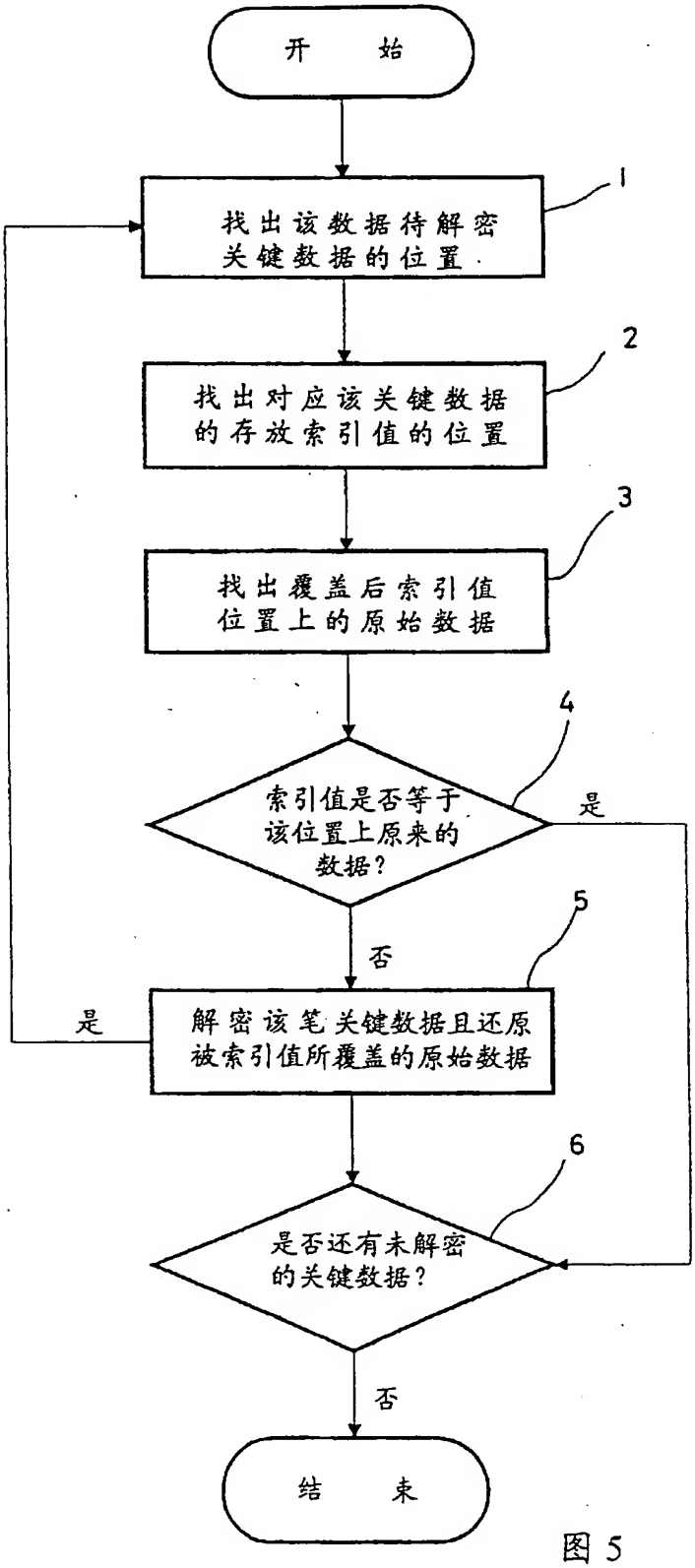

开　始
找出该数据待解密关键数据的位置
1
找出对应该关键数据的存放索引值的位置
2
找出覆盖后索引值位置上的原始数据
3
索引值是否等于该位置上原来的数据?
4
是
否
解密该笔关键数据且还原被索引值所覆盖的原始数据
5
是
是否还有未解密的关键数据?
6
否
结　束

图 5